# A NEW RISK-INFORMED DESIGN AND REGULATORY PROCESS

by

George E. Apostolakis and Michael W. Golay
Massachusetts Institute of Technology

Allen L. Camp and Felicia A. Durán
Sandia National Laboratories

David Finnicum and Stanley E. Ritterbusch
Westinghouse Electric Company

Presented at the Workshop on
Regulatory Challenges for Future Nuclear Power Plants
Advisory Committee on Reactor Safeguards
US Nuclear Regulatory Commission
Washington, DC

## OVERVIEW

In a project funded by the U.S. Department of Energy (USDOE) in its Nuclear Energy Research Initiative Program, the authors have been involved in formulating a new risk-informed approach for nuclear safety regulation. We believe that this work is important because a new regulatory treatment is needed both for the licensing of new non-light water reactors (LWRs), and to rationalize the regulation of LWRs. It is common today for the plans for new reactor concepts to include proposals for how they should be licensed. The existence of such proposals is implicit evidence that the existing regulatory structure is inadequate for this purpose. Similarly, attempts to "risk inform" the regulations governing LWRs have made only small progress because of the complexity and inconsistency of the existing structure. Thus, we have concluded that a fresh start in formulating a regulatory structure is worth attempting. This paper describes the fundamental concepts of that attempt.

The overall purpose of the new approach, termed Risk-Informed Regulation, is to formulate a method of regulation that is logically consistent and devised so that both the reactor designer and regulator can work together in obtaining systems able to produce economical electricity safely. In this new system the traditional tools (deterministic and probabilistic analyses, tests and expert judgement) and treatments (defense-in-depth, conservatism) of safety regulation would still be employed, but the logic governing their use would be reversed from the current treatment. In the new treatment, probabilistic risk analysis (PRA) would be used as the paramount decision support tool, taking advantage of its ability to integrate all of the elements of system performance and to represent the uncertainties in the results. The latter is the most important reason for this choice, as the most difficult part of safety regulation is the treatment of uncertainties, not the assurance of expected performance.

## STRUCTURE OF THE NEW REGULATORY APPROACH

The scope of the PRA would be made as large as that of the reactor system, including all of its performance phenomena. The models and data of the PRA would be supported by deterministic analytical results, and data to the extent feasible. However, as in the current regulatory system, the models and data of the PRA would require being complemented by subjective judgements where the former were inadequate. All of these elements play important roles in the current decision-making structure; the main departure from current practice would be making all of these treatments explicit within the PRA, therefore, decreasing the frequency of sometimes arbitrary judgments.

In the intended sense the PRA would be used as a vehicle for stating the beliefs of the designer and regulatory decision-maker; the foundation of their decisions. Thus, the PRA should be viewed as a Bayesian decision tool, and be used in order to take advantage of its capabilities in integration and inclusion of

uncertainties. In order to do this, all regulations must be formulated in terms of acceptable levels of unavailability of essential functions, including an acceptable level of uncertainty (e.g., the acceptability of system performance could be evaluated at a stated confidence level rather than in terms of the mean value as is typical currently).

Implied in this treatment is a hierarchy of acceptable performance goals. At the highest level societal Safety Goals would be used, supported by subgoals formulated at increasingly fine levels of detail as the hierarchical level of the goal would decrease (see Figure1).

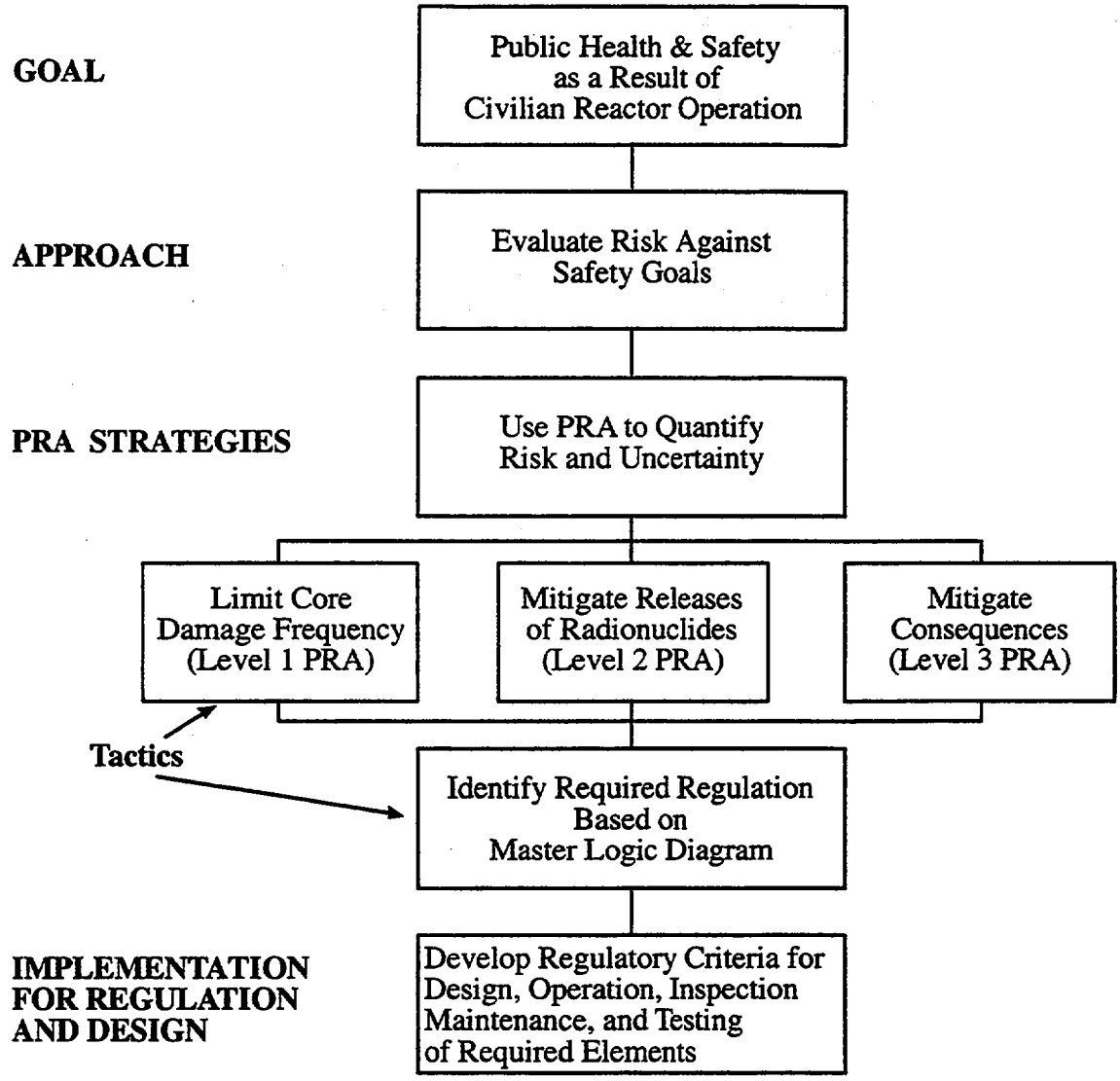



**Figure 1.** Framework for Risk-Based Regulation and Design

The differences between the proposed treatment and current practices are illustrated in Figure 2, which shows that the use of defense-in depth and requiring performance margins would remain. However, the current practice of permitting such features to be required without justification would be abandoned; rather, wherever such a requirement were to be made it would also be necessary for the regulator to provide evidence concerning the value of the requirement and to reflect that value in the master PRA (i.e., if a redundancy is to be worth including in a system, its safety value should also be stated in the overall system performance analysis).

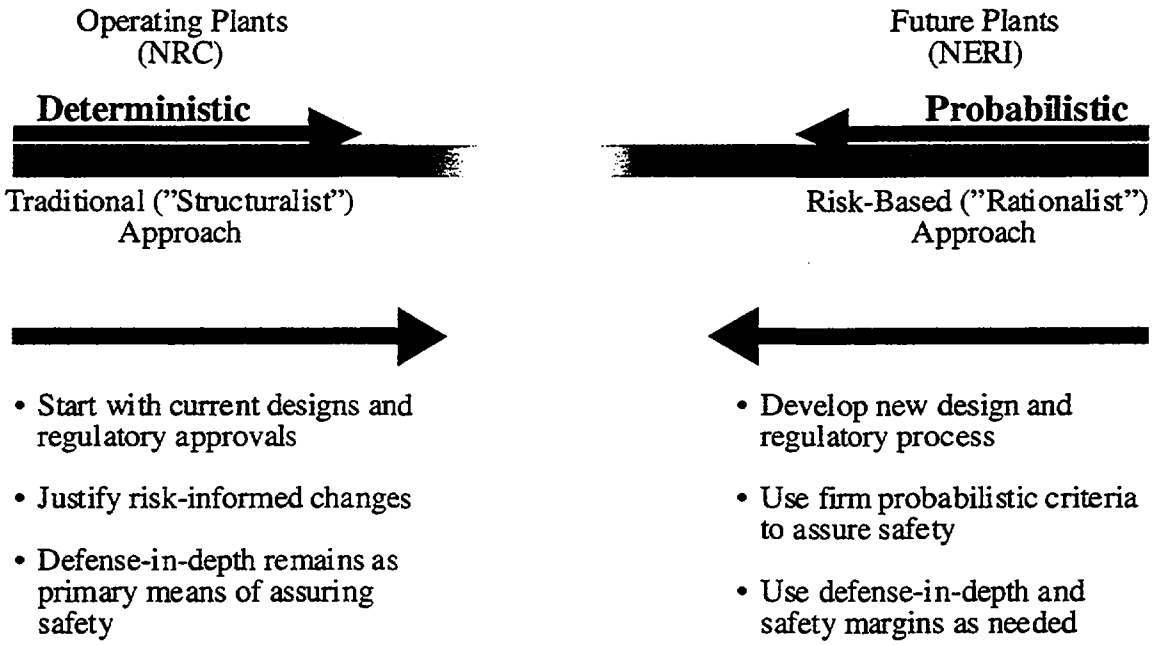



**Figure 2.** Comparison of NRC and NERI Risk-Informed Regulatory Processes

## IMPLEMENTATION

In the licensing of any new reactor concept the degree of detail that the regulatory system may require will increase with the maturity of the concept (see Figure 3). When viewed from this perspective, it is seen that many aspects of the current LWR-focused system of safety regulation (e.g., general design criteria, design basis accidents) may not be applicable as the body of knowledge and experience needed for the formulation of new concepts will likely be unavailable in the earlier stages of their maturation. It is important to realize this in order that un-critical application of current requirements (e.g., a reactor containment building) not lead to impaired system performance or economically inefficient uses of resources. We suggest that some aspects of LWR-based regulation should not be applied to new reactor concepts without careful study.

As far as we can tell, the proposed regulatory approach can be applied to all areas of nuclear safety regulation (see Figure 4), including the "cornerstones" of the NRC's revised reactor oversight process. In the work of our project, we have focused upon the traditional areas of reactor licensing: determination of initiating events and requirements for mitigating systems, but nothing that we have done indicates an inability to extend the ideas being developed to all areas of regulation.

Determination of acceptable unavailability standards for a reactor's essential performance functions must be done on both combined general (high level) and reactor concept-specific bases (see Figure 5). The Master Logic Diagram (MLD) of Figure 5 is developed for the example of the pebble bed modular gas-cooled

*reactor (PBMR). At each level of the MLD a set of performance goals must be* formulated which are required to be consistent with those of the MLD levels immediately above and below the level of interest.

| Development Stage | Goals and Acceptance Criteria | Evaluation Tools | Relevant Evidence |
|---|---|---|---|
| Initial Concept | High level - qualitative | Qualitative, simple, deterministic | Experiences of other concepts, deterministic analyses |
| Initial detailed design | High level - quantitative | Quantitative – probabilistic, deterministic | Prior quantitative analyses |
| Final detailed design | Detailed – quantitative (design-specific subgoals) | Detailed – quantitative – probabilistic, deterministic | Prior quantitative analyses |
| N-th of a kind for a given plant type | Very detailed – quantitative (design specific criteria – DBAs, GDCs,....) | Very detailed – quantitative, probabilistic, deterministic, tests | Prior quantitative analyses, tests, field experience |

**Figure 3.** Stages of Nuclear Power Plant Concept Development

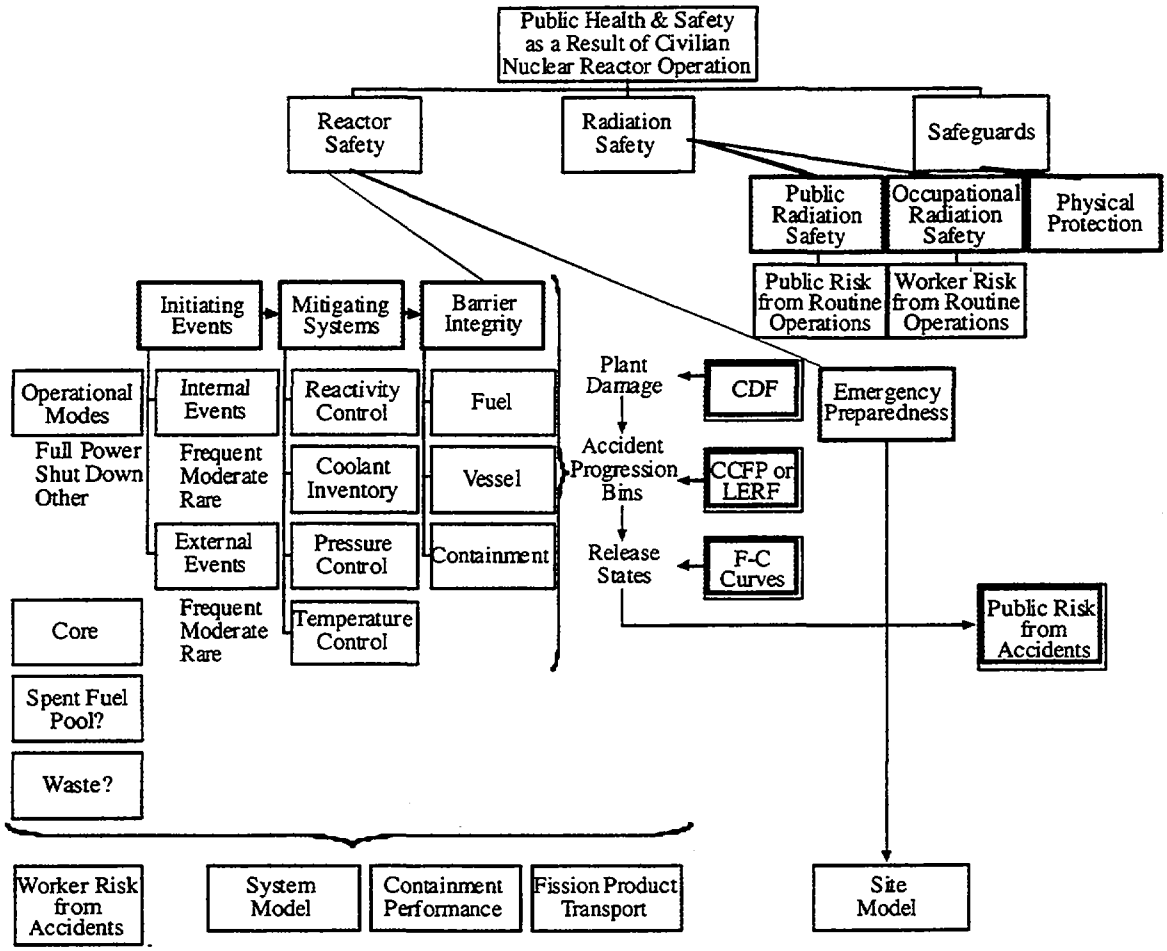



**Figure 4.** Scope of New Regulatory Scheme

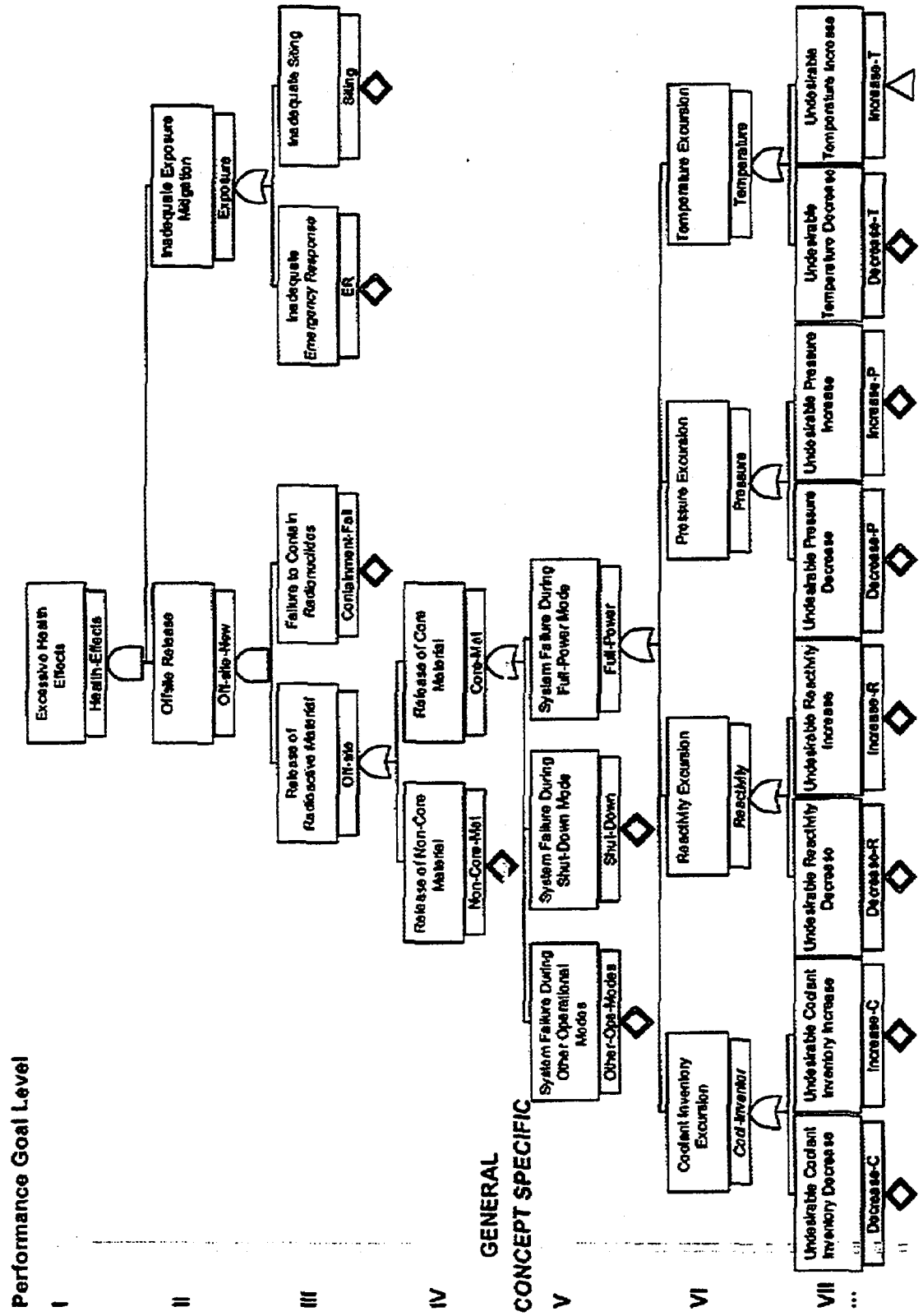



**Figure 5.** Illustrative Logic Diagram for Pebble Bed Modular Gas-Cooled Reactor

In the regulatory example used subsequently to illustrate the practicality of the ideas presented here an acceptable performance goal for all loss of coolant accidents (LOCAs) was formulated to be that

(0.75*CDF-50) + (0.25*CDF-95) < 7 E-7 (per reactor year), where (1)

CDF-50 is the median core damage frequency for all LOCAs, and
CDF-95 is the 95% confidence level value of the core damage frequency for all LOCAs.

This value and its formulation are used merely for purposes of illustration. A method for determination of the various performance goals must be developed. Doing this will likely be an iterative process exploring what is feasible balancing ideals and practicality.

Because new reactor regulation (i.e., licensing) must be able to address the performance vector of different reactor concepts and to accommodate their respectively differing levels of knowledge, the probabilistically-based treatment suggested here appears to be appropriate. For regulation of actual construction and operations it appears to be more feasible to utilize deterministic decision rules, based upon the plant's PRA, and revised as needed via use of the PRA.

## DESIGN AND LICENSING NEGOTIATIONS

In any licensing regulatory process the plant's designer develops a design which he/she considers to be adequate for producing electricity safely. In areas where performance uncertainties are large or where potential accident consequences so large that risk aversion is justified, the designer would have obvious incentives to utilize defense in depth and performance margins in the design, and to reflect the effects of these tactics in the evaluated performance of the plant systems. When this design is submitted for regulatory approval, a negotiation follows which leads to any design changes required for regulatory approval. Currently, this negotiation is conducted focusing upon how adequately the design basis accidents are mitigated, with some background consideration being given to the important risk contributors and risk sensitivities of the plant. In our new design and regulatory concept, this negotiation would be conducted using the PRA as the primary discussion vehicle. The important questions would concern whether the relevant functional performance goals were satisfied with sufficient confidence.

Once the goals were specified, the remaining questions would concern the models and data used in evaluation of the un-availabilities (including uncertainties) associated with performance of these functions. Disagreements between the licensee and regulator would be focused upon the adequacy of models and data used in the PRA. A response to such a disagreement could include further defense in depth or design conservatism, but it could also include defense and improvements of the relevant models and databases.

An additional feature of this approach is that the burden upon the regulator to justify his challenges to the adequacy of the design would be made explicitly. Any design changes that the regulator thinks necessary would also be required to be reflected in the PRA, and the reasons for disagreement about the adequacy of the design would have to be formulated in terms of the adequacy of the PRA. Unavoidably, some of these disagreements would involve factors of subjective judgement. Such judgements would be required to be integrated into the results of the PRA, and their bases stated explicitly. This requirement would be an important departure from current practice where the regulator is not required to justify changes demanded of a license applicant.

For example, in the recent Design Certification licensing of the AP-600 PWR concept, the Certification was held up by the NRC until the designers agreed to add an active containment spray system which is redundant to the passive containment cooling system of the original design. Neither the PRA nor the deterministic design analysis of the plant indicated the need for the active system, but the regulator was able to require that it be added (presumably because of concern that the passive system might display unanticipated modes of behavior) without explicit justification (it was deemed to be the "prudent" thing to do).

As an illustration of how the new negotiation process would work, the designer before application submission would follow the process illustrated in Figure 6. In this process the designer would be guided by the PRA in identifying the set of marginally most valuable design changes to reduce functional unavailability values to being lower than those specified in regulations to be acceptable. The method of doing this would be to search for event sequences where design modifications would best reduce risks and/or their associated uncertainties. Then, once an adequate design is developed it would be submitted for licensing approval.

An illustration of this process is shown in Figure 7. In this illustration, a design thought to be adequate by the designer is rejected by the regulator who disagrees with data and models used to evaluate the risks of high pressure LOCA event sequences in the PRA. Rather than defend the models and data of that portion of the PRA the designer investigates further design changes as summarized in Table 1 and Figure 8. It is seen that addition of greater depressurization capability (used to transform the high pressure LOCA into a low pressure one, for which adequate mitigation systems exist in the design) is inadequate to meet the specified performance goal because of the remaining risk contributions of common cause failures in the emergency diesel generator and cooling water systems. Only when design changes to reduce the risks contributed by the common cause failures does the design become satisfactory to the regulator.

In this illustration, both the designer and regulator become focused upon ways to reduce risks and uncertainties, all of which are stated explicitly. Both parties have incentives to utilize good design practices, high quality components and

redundancy and conservatism in order to ensure that the specified performance goals will be satisfied.

From this examination it is not apparent that tools of current regulation such as design basis accidents and general design criteria are required. They may be retained in regulation for purposes of convenience, but their necessity is not apparent.

Rather, the needs of the new regulatory process are more concerned with ways of formulating a consistent set of performance goals and sub-goals, of ensuring that data bases and models will be of high and uniform quality, of formulating methods for the reproducible integration of subjective judgments into PRAs and for formulation of a risk-based Standard Review Plan for use by the regulatory staff. The tactics for creating some of these needed elements is not obvious as the problems involved are complex and subtle.

The best way of satisfying the new regulatory needs appears to be investigation of a set of example regulatory examples, where needed improvements in a general approach can be revealed via inadequacies in the application. Doing this is time consuming and expensive. Thus, the program for such investigations must be initiated well in advance of the time of anticipated license applications for new reactors and be sustained financially. These requirements imply the need for a program of risk-based regulatory development to be an essential component of any national effort to provide new nuclear power technology options.

The question facing energy technology planners is not that of whether to include a regulatory research component in future nuclear technology development efforts, but rather is one of how to make such an element sufficiently effective that it will permit the creation of the logically consistent and economically efficient licensing process required for the success of future generations of nuclear power technologies. The active participation of the NRC in this process is also essential for its success.

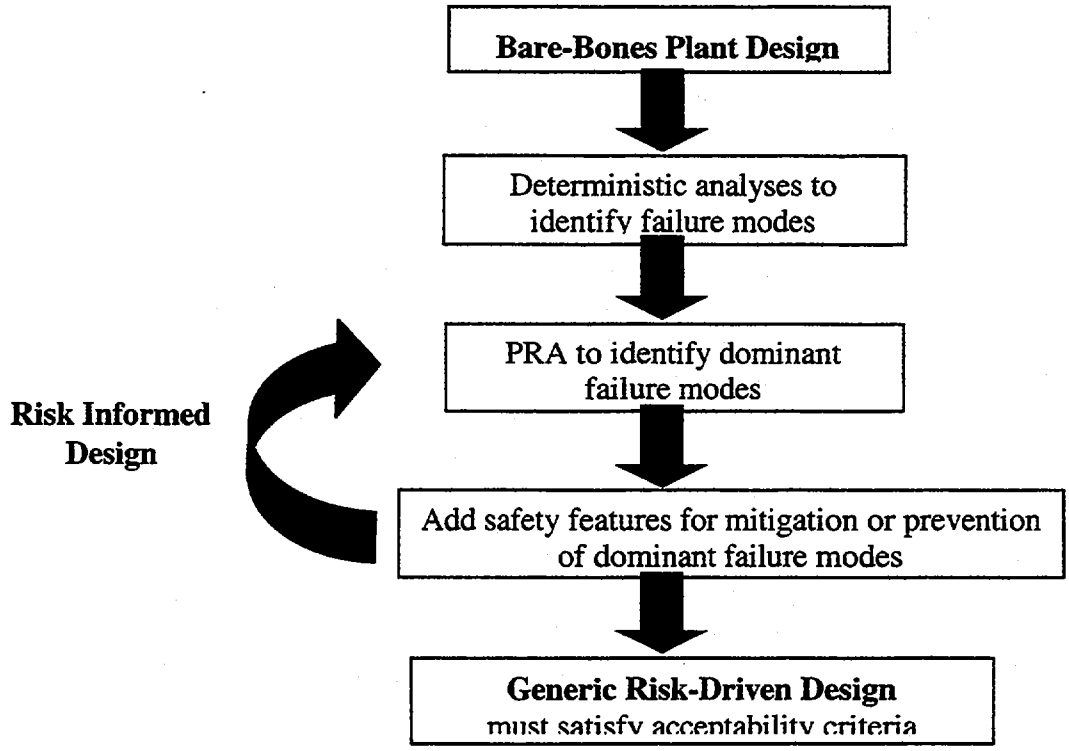



**Figure 6.** Schematic Diagram of the Risk-Driven Generic Design—Builds Upon A Bare-Bones Design, Using an Iterative Process

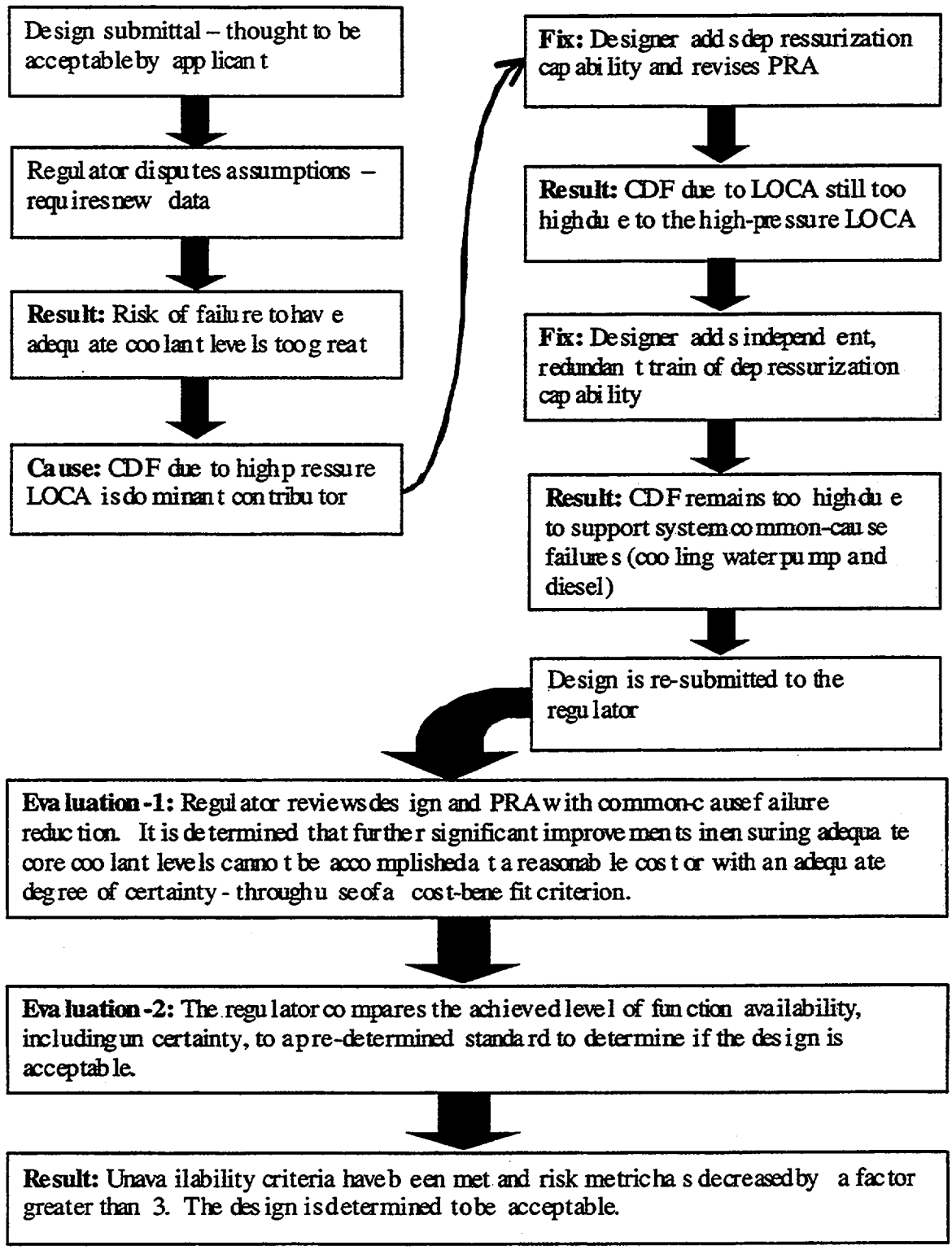



**Figure 7.** Example of Negotiation Between Applicant and Regulator

**Table 1.** Following the Effect of Design Modifications Upon Important Risk Metric Values

| Plant Configuration | Median-CDF | 5% Conf. | 95% Conf. | Risk Metric* |
|---|---|---|---|---|
| No Depressurization | *1.528E-06* | *3.093E-07* | *4.278E-06* | *2.216E-06* |
| One Division of Depressurization | *7.086E-07* | *1.226E-07* | *1.890E-06* | *1.004E-06* |
| Two Divisions of Depressurization | *7.055E-07* | *1.445E-07* | *1.980E-06* | *1.024E-06* |
| Depressurization and reduced CW CC Failure** | *4.970E-07* | *1.008E-07* | *1.432E-06* | *7.308E-07* |
| Depressurization and reduced Diesel CC Failure | *6.120E-07* | *1.211E-07* | *1.718E-06* | *8.885E-07* |
| Depress with reduced CW and Diesel CC Failure | *4.020E-07* | *7.960E-08* | *1.290E-06* | ***6.24E-07*** |

* Risk metric selected = (0.75 □ Median CDF) + (0.25 □ 95% confidence CDF)
** CW = Cooling Water; CC = Common Cause

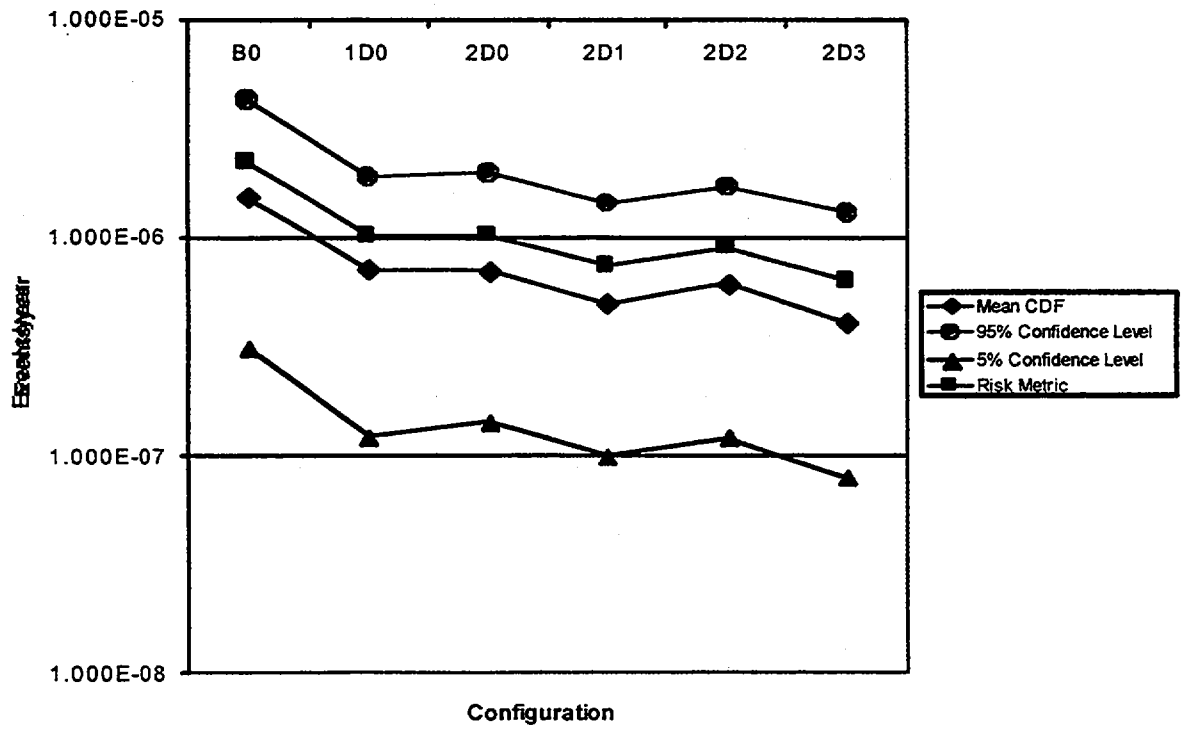



**Figure 8.** Effects of Design Modifications on CDF

# ACRS Workshop on Regulatory Challenges for Future Nuclear Power Plants

## NERI Project on Risk-Informed Regulation

June 5, 2001

Mr. George Davis - Westinghouse
Professor Michael Golay - MIT



## Presentation Breakdown

- Mr. George Davis
  - Purpose and Overview
  - Expectations for the Future
- Professor Michael Golay
  - A New Risk-Informed Design and Regulatory Process
  - Example Problem

Westinghouse
INEEL
Massachusetts Institute of Technology
Duke Engineering & Services
Sandia National Laboratories
NC STATE UNIVERSITY
EGAN & ASSOCIATES, P.C. Counselors at Law

## Purpose of Presentation

- Describe our project and its vision of a new design and regulatory process
  - provide a "work-in-progress" illustrative example
- Explain the need for continuing the development of a new design and regulatory process
  - keep pace with the development and licensing of new reactor design concepts.



## Substantial Reductions in Capital Costs and Schedule Will be Needed for New Plants

- Production costs (Fuel plus O&M) for operating plants approaching 1 cent/KW-hr
  - not much room for further improvement
- Future investors likely to require payback of capital costs within 20 years of operation, or less
- Capital costs must be reduced by 35% or more relative to large ALWRs
  - overnight capital cost below $1,000/KWe
  - construction schedule of about 3 years (or less)

## Three NERI Proposals Aimed at New Processes to Lower Plant Capital Costs

| Program | Basic Objective |
|---|---|
| Risk-Informed Assessment of Regulatory and Design Requirements | Development of methods for a new design and regulatory process. |
| "Smart" Equipment and Systems to Improve Reliability and Safety in Future Nuclear Power Plants | Development of methods for demonstrating improved component and system reliability; including on-line health monitoring systems. |
| Development of Advanced Technologies for Design, Fabrication, and Construction of Future Nuclear Power Plants | Development of methods and procedures for collaborative, internet-based engineering, integrated design analyses, and improved construction schedules. |



## Comparison of NRC and NERI Risk-Informed Regulatory Processes


**The new design and regulatory process must be developed further to support new plant license applications - including Generation IV design concepts.**

## Risk-Informed Assessment - Interactions With Other Programs

- NERI framework development activities are being coordinated with NEI
  - NEI will emphasize the development of regulations
  - The NERI project will address the overall risk-informed design and regulatory process
  - Westinghouse will be an NEI Task Force member
- It is anticipated that a new risk-informed design and regulatory process will be an input to new plant license applications, including Generation IV reactor concepts.



## A New Risk-Informed Design and Regulatory Process

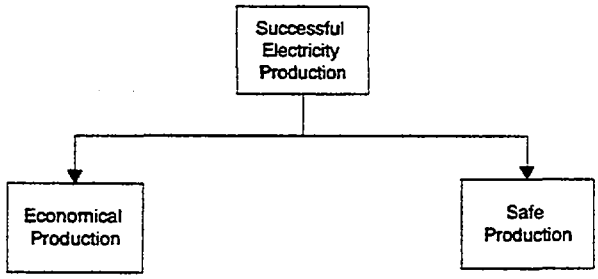
**Massachusetts Institute of Technology**
George Apostolakis, Michael Golay

**Sandia National Laboratories**
Allen Camp, Felicia Durán

**Westinghouse Electric Company**
David Finnicum, Stanley Ritterbusch

## Overall Goal of Safety-Regulatory Reform

- Create methods to assure consistency of nuclear power plant applicant and regulator in performance/ goals for producing safe, economical power plants



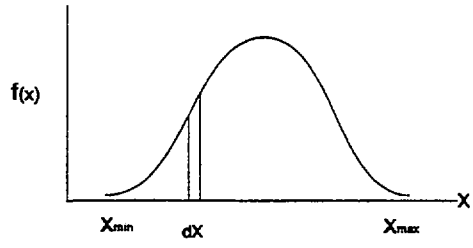

**Major Elements:**
- Acceptance Criteria
- Comprehensive, consistent assessment methods
- Designers, operators

**Major Elements:**
- Acceptance Criteria
- Comprehensive, consistent assessment methods
- Regulators, designers, operators



## Risk-Informed Regulatory Approach - Fundamental Ideas

- Regulatory decisions are founded upon the informed beliefs of decision-makers.
- Any regulatory belief can and should be stated in a probabilistic format.



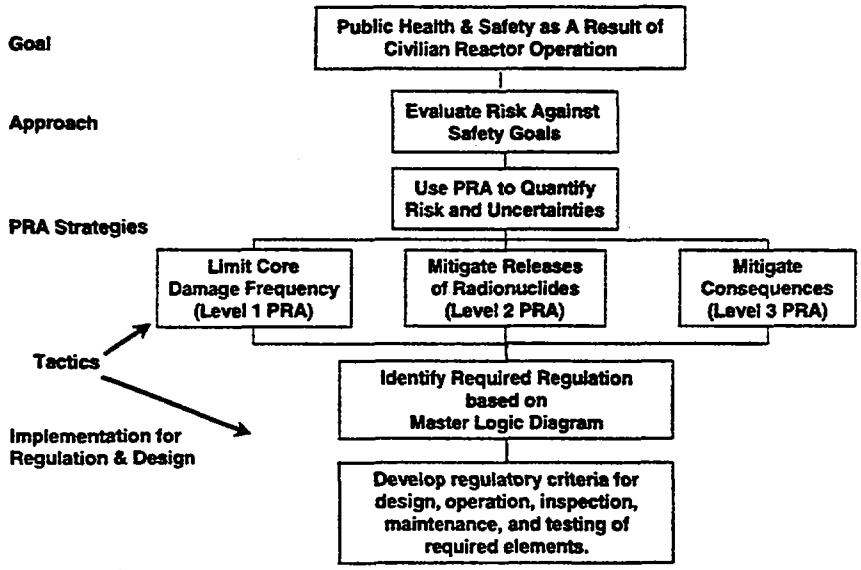

Probability $(x < X < x+dx) = f(x)dx$

- Regulatory acceptance criteria must reflect acceptable best-estimate performance expectations and uncertainties.

# Risk-Informed Regulatory Approach - Fundamental Ideas....

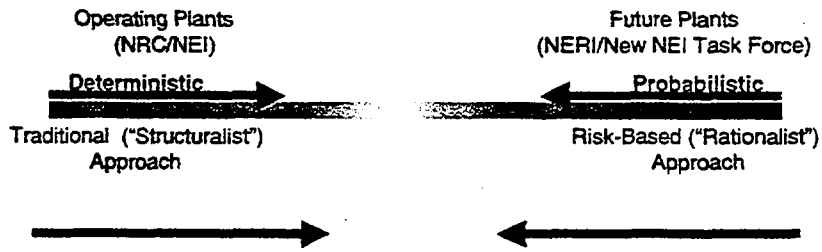
- Regulatory questions and acceptance criteria should also be stated within a probabilistic framework.
- The probabilistic framework should be as comprehensive as possible:
  - utilize probabilistic and deterministic models and data where feasible - and use subjective treatments where not feasible,
  - state all subjective judgments probabilistically and incorporate into the PRA,
  - require both license applicant and regulatory staff to justify their decisions explicitly, and
  - initiate resolution process to resolve applicant-regulator disagreements.






**Framework for Risk-Based Regulation and Design**

# Comparison of NRC and NERI Risk-Informed Regulatory Processes




- Start with current designs and regulatory approvals.
- Justify risk-informed changes.
- Defense-in-depth remains as primary means of assuring safety.

- Develop new design and regulatory process.
- Use firm probabilistic criteria to assure safety.
- Use defense-in-depth and safety margins as needed.



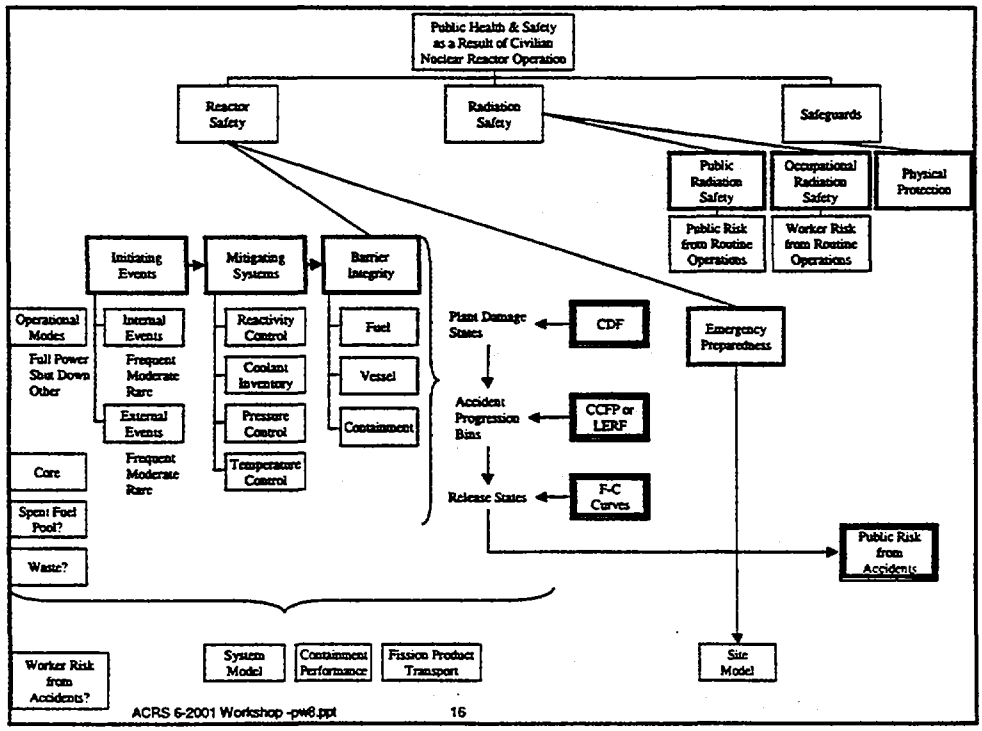
# Risk-Informed Regulatory Approach....

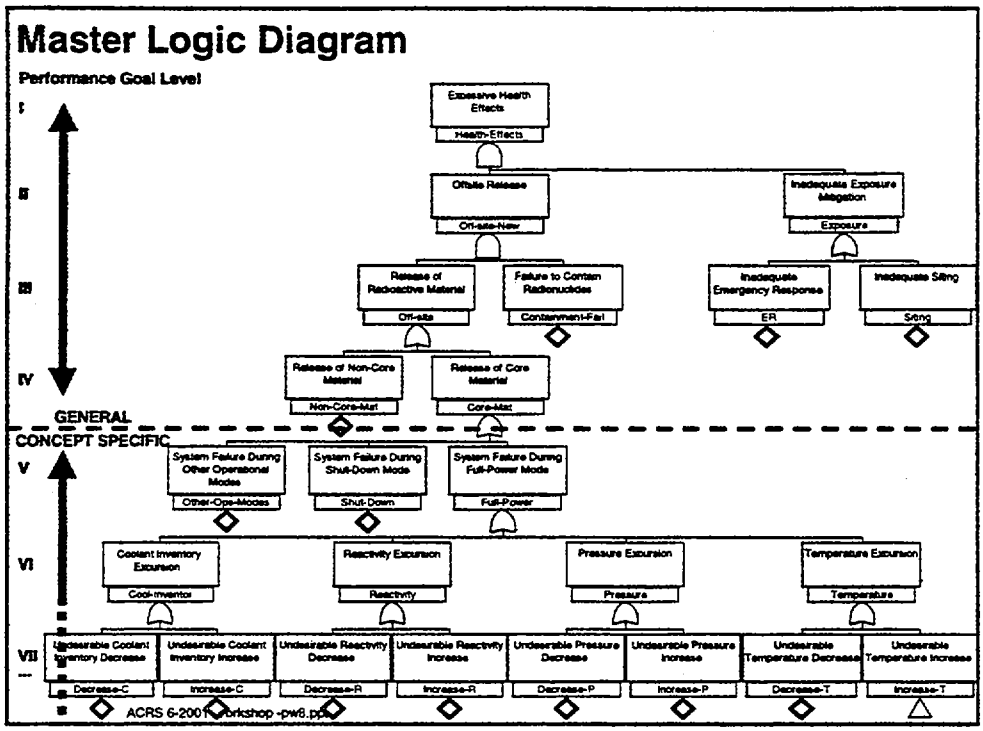
- At all conceptual stages of development, nuclear power plant evaluation is performed probabilistically and is supported by deterministic analyses, tests, experience, and judgements.
- Safety results of defense-in-depth, performance margins, best-estimate performance, and subjective judgements are all incorporated into a comprehensive PRA
  - PRA is used as a vehicle for stating evaluator beliefs concerning system performance
- The level of detail of acceptance criteria becomes finer as the level of concept development increases
  - many LWR-based regulatory constructs (e.g., DBAs, GDCs) are not applicable to less mature

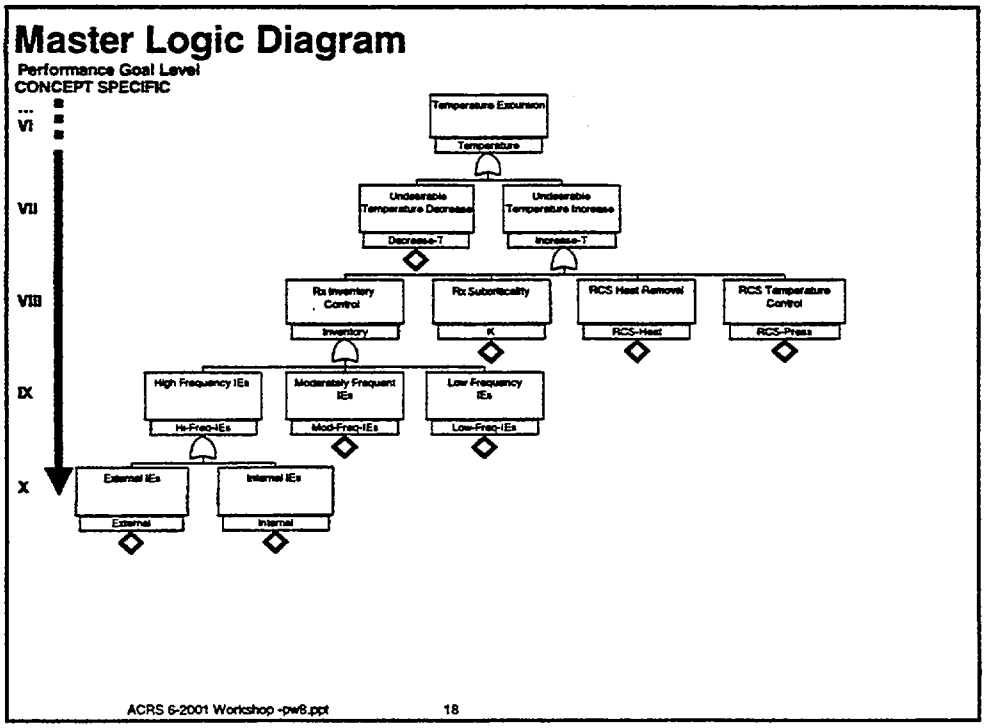
## Stages of Nuclear Power Plant Concept Development

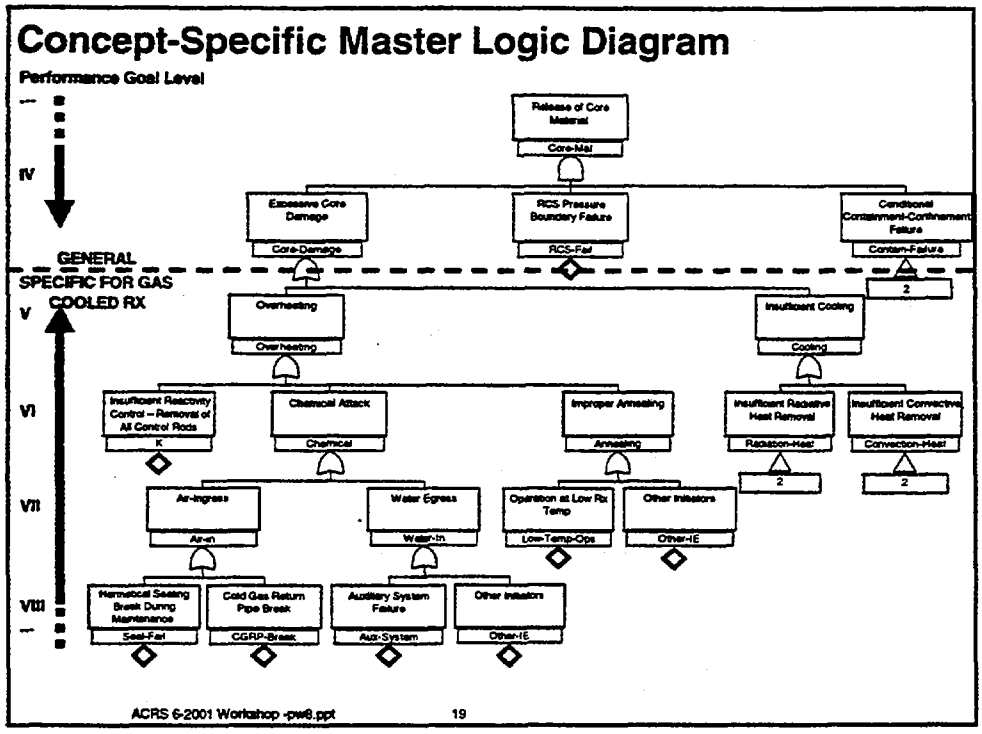
| Development Stage | Goals and Acceptance Criteria | Evaluation Tools | Relevant Evidence |
|---|---|---|---|
| Initial Concept | High level - qualitative | Qualitative, simple, deterministic | Experiences of other concepts, deterministic analyses |
| Initial detailed design | High level - quantitative | Quantitative – probabilistic, deterministic | Prior quantitative analyses |
| Final detailed design | Detailed – quantitative (design-specific subgoals) | Detailed – quantitative – probabilistic, deterministic | Prior quantitative analyses |
| N-th of a kind for a given plant type | Very detailed – quantitative (design specific criteria – DBAs, GDCs,....) | Very detailed – quantitative, probabilistic, deterministic, tests | Prior quantitative analyses, tests, field experience |

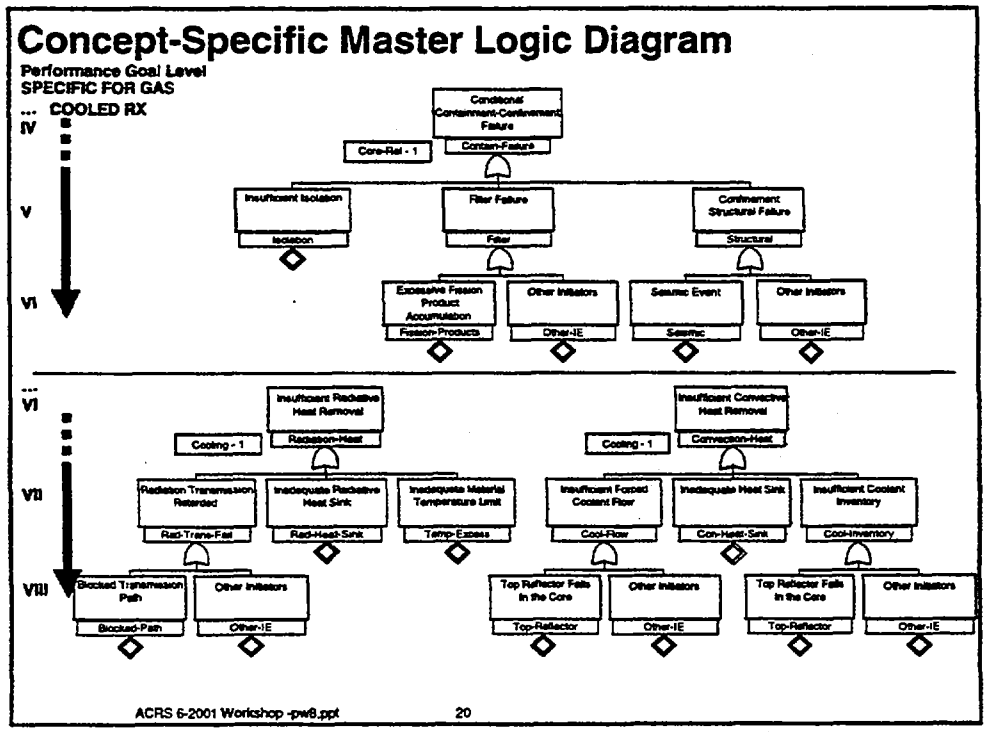





Master Logic Diagram
Performance Goal Level
I
II
III
IV
GENERAL
CONCEPT SPECIFIC
V
VI
VII
Excessive Health Effects
Health-Effects
Offsite Release
Off-site-Rel
Inadequate Exposure Mitigation
Exposure
Release of Radioactive Material
Off-site
Failure to Contain Radionuclides
Containment-Fail
Inadequate Emergency Response
ER
Inadequate Siting
Siting
Release of Non-Core Material
Non-Core-Mat
Release of Core Material
Core-Mat
System Failure During Other Operational Modes
Other-Ops-Modes
System Failure During Shut-Down Mode
Shut-Down
System Failure During Full-Power Mode
Full-Power
Coolant Inventory Excursion
Cool-Inventor
Reactivity Excursion
Reactivity
Pressure Excursion
Pressure
Temperature Excursion
Temperature
Undesirable Coolant Inventory Decrease
Undesirable Coolant Inventory Increase
Undesirable Reactivity Decrease
Undesirable Reactivity Increase
Undesirable Pressure Decrease
Undesirable Pressure Increase
Undesirable Temperature Decrease
Undesirable Temperature Increase
Decrease-C
Increase-C
Decrease-R
Increase-R
Decrease-P
Increase-P
Decrease-T
Increase-T
ACRS 6-2001 Workshop -pw8.ppt


Master Logic Diagram
Performance Goal Level
CONCEPT SPECIFIC
VI
VII
VIII
IX
X
Temperature Excursion
Temperature
Undesirable Temperature Decrease
Undesirable Temperature Increase
Decrease-T
Increase-T
Rx Inventory Control
Rx Subcriticality
RCS Heat Removal
RCS Temperature Control
Inventory
K
RCS-Heat
RCS-Press
High Frequency IEs
Moderately Frequent IEs
Low Frequency IEs
Hi-Freq-IEs
Mod-Freq-IEs
Low-Freq-IEs
External IEs
Internal IEs
External
Internal
ACRS 6-2001 Workshop -pw8.ppt
18


Concept-Specific Master Logic Diagram
Performance Goal Level
IV
GENERAL
SPECIFIC FOR GAS COOLED RX
V
VI
VII
VIII
Release of Core Material
Core-Mel
Excessive Core Damage
Core-Damage
RCS Pressure Boundary Failure
RCS-Fail
Conditional Containment-Confinement Failure
Contain-Failure
2
Overheating
Overheating
Insufficient Cooling
Cooling
Insufficient Reactivity Control – Removal of All Control Rods
K
Chemical Attack
Chemical
Improper Annealing
Annealing
Insufficient Radiative Heat Removal
Radiation-Heat
Insufficient Convective Heat Removal
Convection-Heat
Air-Ingress
Air-In
Water Egress
Water-In
Operation at Low Rx Temp
Low-Temp-Ops
Other Initiators
Other-IE
Hermetical Sealing Break During Maintenance
Seal-Fail
Cold Gas Return Pipe Break
CGRP-Break
Auxiliary System Failure
Aux-System
Other Initiators
Other-IE
ACRS 6-2001 Workshop -pw8.ppt
19


Concept-Specific Master Logic Diagram
Performance Goal Level
SPECIFIC FOR GAS
... COOLED RX
IV
V
VI
VII
VIII
Conditional Containment-Confinement Failure
Core-Rel - 1
Contain-Failure
Insufficient Isolation
Isolation
Filter Failure
Filter
Containment Structural Failure
Structural
Excessive Fission Product Accumulation
Fission-Products
Other Initiators
Other-IE
Seismic Event
Seismic
Other Initiators
Other-IE
Insufficient Radiative Heat Removal
Radiation-Heat
Cooling - 1
Insufficient Convective Heat Removal
Convection-Heat
Cooling - 1
Radiation Transmission Retarded
Rad-Trans-Fail
Inadequate Radiative Heat Sink
Rad-Heat-Sink
Inadequate Material Temperature Limit
Temp-Exces
Insufficient Forced Coolant Flow
Cool-Flow
Inadequate Heat Sink
Con-Heat-Sink
Insufficient Coolant Inventory
Cool-Inventory
Blocked Transmission Path
Blocked-Path
Other Initiators
Other-IE
Top Reflector Fails in the Core
Top-Reflector
Other Initiators
Other-IE
Top Reflector Fails in the Core
Top-Reflector
Other Initiators
Other-IE
ACRS 6-2001 Workshop -pw8.ppt
20

## Fundamental Interactions Between License Applicant (or Licensee) and Regulator

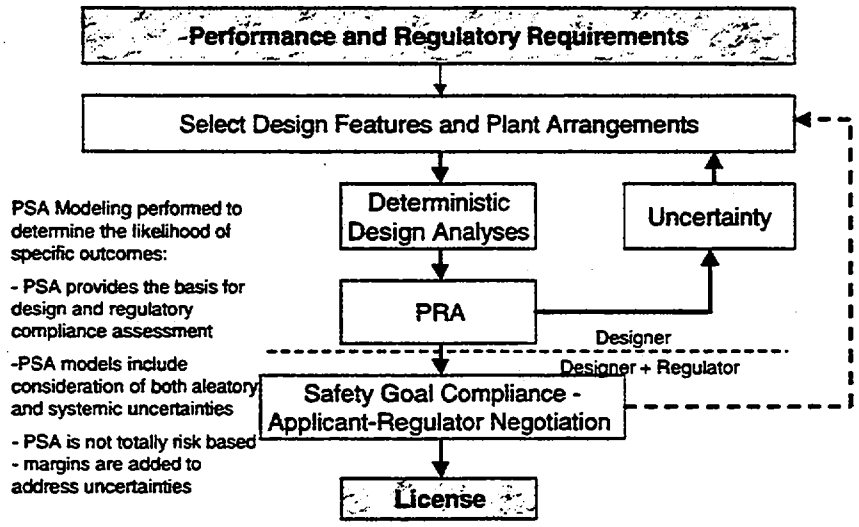
- Should be formulated with probabilistic methods
- Acceptability negotiation for new license application or license revision
  - currently is deterministic
  - should be risk-based; completion of procedures, tools, and termination criteria is needed
- Plant construction oversight
  - can be deterministic, subject to risk-based oversight
- Plant operation oversight
  - can be deterministic, subject to risk-based oversight



## Basic Design and Regulatory Process - Employed Traditionally, Remains Valid Today

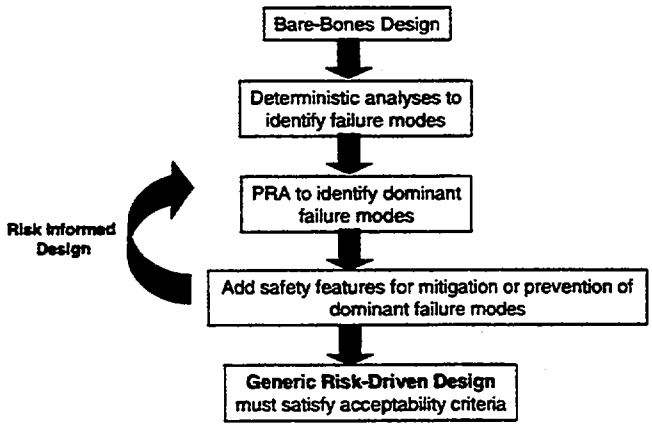
- Designer develops a plant design that both produces power reliably and operates safely
  - responsible for plant safety, using high level regulatory criteria and policies as inputs
- Regulator reviews the design
- Designer and regulator engage in a dialog
  - specific safety features, their performance criteria, and methods of design and analysis
- Documentation is developed throughout the process
  - designer documents the design basis
  - regulator documents the safety evaluation, policies established, and criteria for future reviews (e.g., Reg. Guides and Standard Review Plans, and possibly regulations)

# Risk-Informed Design and Regulatory Process - PRA Decision Making

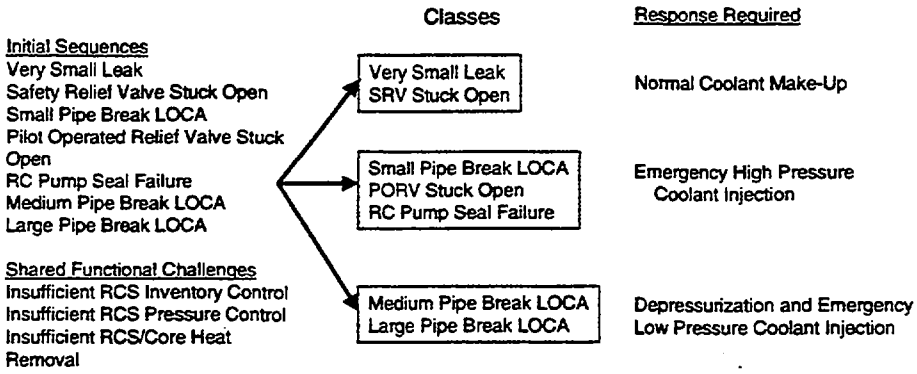





# Schematic Diagram of the Risk-Driven Generic Design - Builds Upon A Bare-Bones Design, Using an Iterative Process



# Classification of Event Sequences Within the Risk-Informed DBA Approach






# Apportionment of a Performance Goal Into Subgoals

- Designer proposes apportionment - then negotiates with regulator
- Apportionment must reflect what is feasible in the design
- Example shows that the reliability/availability of mitigation systems reflects feasibility of the design

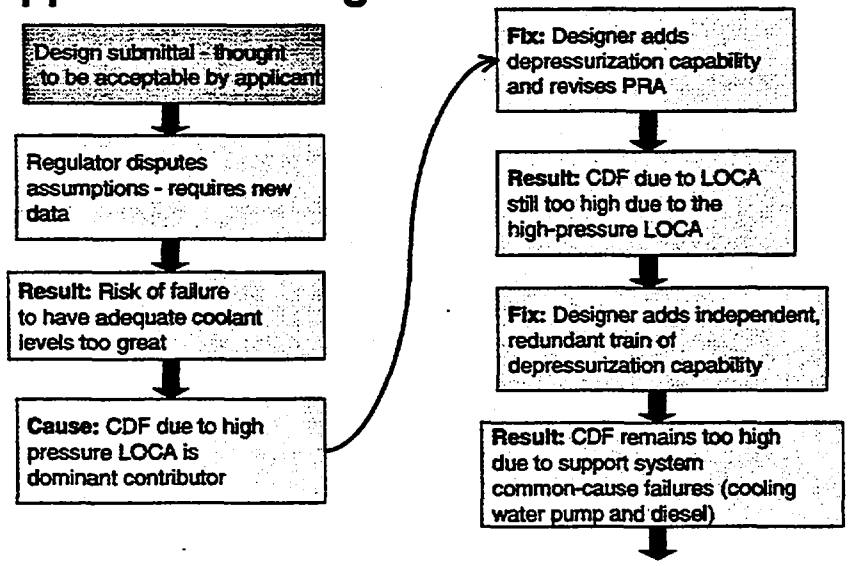
| Initiating Event | Initiating Event Frequency | Mitigation Unavailability | Core Damage Frequency |
|---|---|---|---|
| Very Small LOCA | 4E-3 /yr | 1E-4 | 4E-7/yr |
| Small LOCA | 2E-4 /yr | 1E-3 | 2E-7/yr |
| Large LOCA | 4E-5 /yr | 1E-2 | 4E-7/yr |
| Example Acceptability Criterion: Achieved Total CDF due to LOCAs must be less than or equal to **2E-6 /yr** | | | Achieved Total CDF due to LOCAs: **1E-6 /yr** |

# Example of Designer's Initial Risk-Informed Submittal to the Regulator

- Two safety system divisions - each contains:
  - two active high-pressure injection trains
  - one active low-pressure injection train
  - cooling water (component cooling, service water, HVAC)
  - two diesel generators
  - DC (battery) power
- Shared support systems
  - chemical volume control system
  - off-site power
- PRA Includes:
  - deterministic analyses, data, models,
  - uncertainties, inter-dependencies, and common-cause failures
  - initiator data are from documented sources (NUREG/CR-5750)
  - component failure frequencies are estimated from existing PRA studies (for this LWR example problem)



# Example of Negotiation Between Applicant and Regulator



# Example of Negotiation Between Applicant and Regulator....

Design is re-submitted to the regulator

**Evaluation-1:** Regulator reviews design and PRA with common-cause failure reduction. It is determined that further significant improvements in ensuring adequate core coolant levels cannot be accomplished at a reasonable cost or with an adequate degree of certainty - through use of a cost-benefit criterion.

**Evaluation-2:** The regulator compares the achieved level of function availability, including uncertainty, to a pre-determined standard to determine if the design is acceptable.

**Result:** Unavailability criteria have been met and risk metric has decreased by a factor greater than 3. The design is determined to be acceptable.



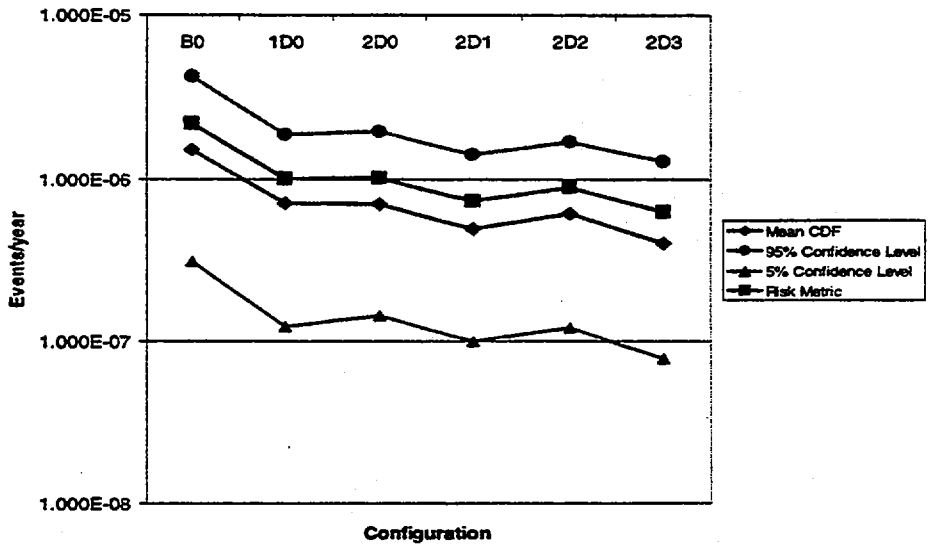
# Following the Effects of Design Modifications Upon Important Risk Metric Values

| Plant Configuration | Median-CDF | 5% Conf. | 95% Conf. | Risk Metric* |
|---|---|---|---|---|
| No Depressurization | *1.528E-06* | *3.093E-07* | *4.278E-06* | *2.216E-06* |
| One Division of Depressurization | *7.086E-07* | *1.226E-07* | *1.890E-06* | *1.004E-06* |
| Two Divisions of Depressurization | *7.055E-07* | *1.445E-07* | *1.980E-06* | *1.024E-06* |
| Depressurization and reduced CW CC Failure** | *4.970E-07* | *1.008E-07* | *1.432E-06* | *7.308E-07* |
| Depressurization and reduced Diesel CC Failure | *6.120E-07* | *1.211E-07* | *1.718E-06* | *8.885E-07* |
| Depress with reduced CW and Diesel CC Failure | *4.020E-07* | *7.960E-08* | *1.290E-06* | ***6.24E-07*** |

* Risk metric selected = (0.75 * Median CDF) + (0.25 * 95% confidence CDF)

** CW = Cooling Water; CC = Common Cause

# Effects of Design Modifications on CDF






# Example Problem - Results & Questions

- Concerns about common cause failures and large uncertainties would lead designers and regulators to conservative design approaches
  - defense-in-depth, safety margins
- Guidelines are needed for consistently reflecting model weaknesses in the probabilistic database
- Consistent acceptance criteria are needed for negotiation guidance and termination
- Practical implementation requires more work
  - more trial examples
  - standardized models, methods, databases
  - methods for treatment of subjective judgements
  - replacements for:
    - GDCs
    - DBAs (risk-dominant event sequences)
    - Standard Review Plan

## Summary

- The favored approach for a new design and regulatory process would:
  - use risk-based methods to the extent possible
  - use defense-in-depth when necessary to address model and data uncertainty.
- A new risk-informed design and regulatory process would:
  - provide a rational method for both design activities and applicant-regulator negotiations
  - provide a method for an integrated assessment of uncertainties in design and regulation
  - provide a process that is applicable to non-LWR technologies
- Development of a new design and regulatory process should be continued to support new reactor license applications.

**T. Kress, Future Reactors Subcommittee Chairman:** How would you deal with the issue that the PRAs are traditionally very incomplete? They don't deal with shutdown conditions very well. They don't include fires very well, and seismic even is often not treated very well -- would you incorporate those kinds of missing ingredients into the uncertainty of distribution?

**M. Golay:** Yes, basically the way you would incorporate them is through a statement of the subjective judgment of those who have to assess what practice is to be used.

**D. Powers,ACRS Member:** You're going to expand the capability of PRA to carry this out. One of the areas you're going to expand it to carry it out is in the shutdown risk. I presume that you have a plant here that you say is going to have some history, and during that history it's going to have various kinds of shutdowns, those that it planned, to do a variety of activities that are going to be quite different, and it's going to have an occasional unscheduled shutdown. And you can prognosticate all of those things, all of the different configurations of the plant that go on during a shutdown, a scheduled shutdown for refueling and what not. But now we don't try to quantify, those times and configurations, and yet you want us to do that. How is this possible?

**M. Golay, MIT:** I would say that your task in those areas has not changed from that people have today; that when you consider a license application, you try to consider the spectrum of conditions under which the plant will be operated, and using evidence appropriate for each condition, judge whether it will be operated successfully.

The development of shutdown risk analysis provides an illustration of how you do that in, say, a non-power state, and when you're comparing operations between those states, you, as T. Kress just brought out, you inevitably come to situations where the available objective evidence is not sufficient for you to determine which practice is better. Do you do perform maintenance while you're shut down or do you do it on line, for example? Again, subjective judgment has to come into the process. What I'm submitting is that we use that subjective judgment today. We simply don't spell out loud the factors the way that we're weighing the factors. What's changed with the approach that we're suggesting is that we state everything in probabilistic terms and incorporate it into the PRA.

**T. Kress, Future Reactors Subcommittee Chairman:** What I'm interested in is the risk associated over the full lifetime of the plant. That means shutdown number e.g; 85 is going to take place "n" years from now and I need to incorporate into my risk assessment. Now, since I don't know what that shutdown consists of, what planned maintenance they're going to have because it hasn't even come about yet, it may even be an unplanned shutdown. How do I know how to incorporate the short time during shutdown, short compared to other things? That risk, how do I put that risk component into my risk assessment when I don't even know what it is. We're dealing with a change, a variable configuration in time rather than a fixed configuration, which is what PRAs usually deal with. How do I deal with that in a PRA? Is that something that needs a new PRA methodology?

**M. Golay, MIT:** I would submit not, but let me go to why. The first question that may arise is why do you need research on regulatory reform. Why can't you just get a few people to go off and think in the corner for a time and come up with some proposals and then try them out?

My experience has been that you don't know what is a good idea until you've gone through some feasibility attempts. That there's an iterative process at work here, and that's the heart of

regulatory reform research, to find out what's feasible and then from that find a good blend of feasible approaches consistent with an over arching logical framework. In terms of the question you've asked, I would suspect, without having tried to do the analysis, that, first of all, the level of detail that you indicate as being required is probably not necessary; that approaching it from the point of view of looking at safety during shutdown and trying to anticipate a range of conditions that you think are reasonably plausible, which is the approach we have today, will likely work. What I would try and do is turn the question around and try and use a real probabilistic treatment of the safety, but not to try and anticipate the fine detail the history of a plant that might occur or might not occur.

**G. Wallis, ACRS Member:** Do you have a good measure of safety margin in a probabilistic sense?

**M. Golay, MIT:** Yes. If you're using margin on let us say concerning the approach to melting temperature or something of that kind, what that would translate into would be to formulate your acceptance criterion from the design point of view at a very, very high confidence level so that you ensure satisfaction.

**G. Wallis, ACRS Member:** But once you start saying there's a failure point, you are making things deterministic, which really are not.

**M. Golay, MIT:** Well, I'm trying to relate it to the current design process.

**G. Wallis, ACRS Member:** That's right, but I think it would be interesting to see what you could do with a definition of margin which got away from these ideas of having a point or --

**M. Golay, MIT:** Right, and what you would do, as you're hinting, is really to use a distribution on all of the performance limits, and that would be a natural evolution that I think we would go to and probably quicker than I'm anticipating.

**G. Wallis, ACRS Member:** You would look at the probabilities of all of those and the consequences of all of those.

**M. Golay, MIT:** Right. That's right. So what you expect is that if people are using the approach we're suggesting well, they would have natural incentives to put defense-in-depth into their designs partly because they could see a benefit for doing it when they make a regulatory submittal. The same thing would be the case with incorporating performance margin.

**T. Kress, Advanced Reactor Subcommittee Chairman**: How do I decide what confidence level constitutes an acceptable margin?

**M. Golay, MIT:** My short answer is you have to work on it. It's partly a social policy and has to be worked out in an iterative manner.

**G. Wallis, ACRS Member:** It's an interesting idea, but it seems to me that as you learn more about a plant, you might actually get less detail than any kind of plan. You might really know what you have to worry about and you don't need all of this detail.

**M. Golay, MIT:** Conceivably, and we've seen that, for example. The evolution of the passively based water-cooled reactors could be an illustration of that. But one reason for putting this

figure together is to address this question of where do the design basis accidents and general design criteria come into the picture. I would say that it's a tentative conclusion, not a firm one, that those really play a role when you get to the detailed design and later stages of evolution because when you try to formulate design basis accidents, you have to have a design. You have to have a concept in terms of which to think about and have some seasoning in terms of your understanding of its weaknesses, things of that kind. if you look at what we've done with light water reactors, we've gone through that process.

**G. Wallis, ACRS Member:** Let's try to think about this. The method of design and analysis is going to be in probabilistic terms. You mean that every time you put a correlation in a code, you have to do something probabilistic with it?

**M. Golay, MIT:** Only if it propagated through into your risk evaluation.

**G. Wallis, ACRS Member:** It probably does.

**M. Golay, MIT:** Yes. For example, if your new correlation had a different uncertainty treatment, you would expect that to be propagated through. That's right.

**G. Wallis, ACRS Member:** Why do you need subgoals? It seems to me that if you had a plant that had no LOCA probability at all because of its design, then you might trade this off and be allowed to have more probability somewhere else if all you care about is the total.

**M. Golay, MIT:** But you care about the uncertainty associated with the total as well.

**G. Wallis, ACRS Member:** Yes, you do, but the total, the bottom line is the thing, not really how it breaks up in all these pieces.

**M. Golay, MIT:** Well, I would say that another reason why you want to do this is that in the long run for regulatory convenience and efficiency, you probably want to formulate risk-based deterministic decision rules as you reach a high stage of maturity. So there will be sort of natural incentives to formulate subgoals as the concept matures. And that's the reason we have this in here, simply to illustrate that you have to go through this iterative process.

**L.E. Hochreiter, Penn State University:** You talk about using best estimate performance, expectations and uncertainties. And you really have two kinds of uncertainties. You can have the plant uncertainties, but you can have the uncertainties in the model that you use to do the predictions, and with a light water reactor, we've got 40 years of a database, experimental database so that we can quantify the models and the model uncertainty so that we have a good handle on that. I don't know how you address that for a new design like we've been talking about for these Gen. IV designs where you really don't have much of a database at all.

**Mike Golay, MIT:** Yes, with any concept, regardless of its level of maturity, I'll submit that as you try to do a risk analysis of comparing alternatives, you ultimately end up at a point where the available objective data reach their limits. You can find this with plenty of light water examples as well, that what you're really into is a situation where you -- I think always -- that's too strong a word because I don't have the basis for saying "always," but my experience has been so -- that you end up with a combination of objectively based evidence and you have to supplement that by your judgment. So the only suggestion that we're making is that you should state that in probabilistic terms and incorporate it into the PRA so that with the new concept,

you reach that limit much sooner than with the mature one, but that the general structure holds up for both.

**Larry Parme, General Atomics:** You mentioned possibly replacing the DBAs with the risk dominant events, and overall I'm supportive of your approach, but in the licensing risk based approach that we did for the MHTGR, one of the things we were looking at that sort of approach, and we immediately ran into the problem that when you go and say that the risk dominant events replace DBAs, you find that certain non-risk dominant events are the only challenges, if you will, to certain key equipment or safety functions, and the risk dominant events may not demonstrate to the regulator the various ways that your safety functions are done. And I hope you follow what I'm saying. My question to you is: did you think about this?

We had thought about this in the '80s, found that risk dominant events weren't a true substitute for DBAs and had to also use the PRA, but had to find from our event trees events that challenged each of the safety functions regardless of their risk dominance.

**Mike Golay, MIT:** Right. Let me try and translate it though. What I think you're really saying is that there's a concern about the level of uncertainty associated with your risk based analysis, such that if you went in and claimed that you were doing very, very well, it wouldn't be a credible claim, and that it was necessary to, in effect, show that you could handle something tougher, is in some way a defense- in-depth kind of capability.